משרד החינוך
מינהל מדע וטכנולוגיה
מגמת תקשוב

תכנית לימודים – אבטחת מידע

מטרות היחידה

- להקנות מושגי יסוד על מערכות תקשורת מאובטחות.
- ללמוד את מערכות התקשורת ברשת מקומית ורחבה.
- ללמוד דרכים לאבטחת הרשת .
- ליישם את מערכיי האבטחה והצפנות.
- ליישם את מערכיי האבטחה בכדיי לבנות תשתית אבטחה ללקוח .

טבלת הפרקים וחלוקת השעות המוצעת

פרקי הלימוד	עיוני	מעשי
פרק 1 – מבוא לאיומי רשת חדשים	10	0
פרק 2 – אבטחת אביזרי רשת	10	2
פרק 3 – מודל ה AAA	11	3
פרק 4 – חומות אש ברשת הבינונית והרחבה	11	2
פרק 5 – מניעת חדירה לרשת המקומית ורחבה	11	3
פרק 6 – אבטחת הרשת המקומית	11	2
פרק 7 - מערכות הצפנה וקיפטולוגיה	11	3
פרק 8 - מערכות VPN (Virtual Private Network)	10	3
פרק 9 - ניהול אבטחת רשת מתקדם	11	3
סה"כ	**96**	**24**

פרק 1 – מבוא לאיומי רשת חדשים

מטרות :

התלמיד ירכוש ידע על אבולוציית אבטחת המידע
התלמיד ירכוש כלים לאבטחת מידע
התלמיד ירכוש ידע על מערכות והתקפת מערכות

נושאים :

מבוא לאיומי רשת
עקרונות אבטחת הרשת
אבולוציית אבטחת הרשת
אביזרים לאבטחת רשת וסטנדרטים באבטחה
ארגון אבטחת הרשת
תחום אבטחת המידע
התמודדות מול וירוסים סוסים טרויאנים ותולעים
חקר ההתקפות

משרד החינוך
מינהל מדע וטכנולוגיה
מגמת תקשוב

איסוף מידע על התקפות
התקפת מערכות גישה
התקפת מערכות ע"י מניעת שירות (DOS)
שיכוך מתקפות ברוטליות

פרק 2 – אבטחת אביזרי רשת

מטרות :

התלמיד יגדיר ויאבטח את מערכות התקשורת ע"י שימוש ב CLI וב SDM
התלמיד ירכוש כלים לאבטחת מצבי הגישה לאביזרי רשת
התלמיד ירכוש ידע על מערכות syslog, SNMP, SSH, and NTP
ויטמיע אותם במערכת
התלמיד יבדוק את אבטחת מערכות התקשורת ע"י SDM ו Auto Secure

נושאים :

אבטחת נתבי קצה
ניהול חיבורים להגדרות נתבים
ניהול והגדרת חיבורים מרוחקים
הגדרת SSH לגישה מרחוק
הגדרות רמות גישה
OOB ושימוש באמצעי LOGGIN
שרתיי SYSLOG , SNMP , NTP
ביקורת חשבונות
נעילת נתבים לאבטחה מבוקשת
שימוש ב SDM לוריפיקציה

פרק 3 – מודל ה AAA

מטרות :

התלמיד ירכוש ידע על מודל ה AAA
התלמיד ירכוש ידע על שרתי מבוססי מודל ה AAA
התלמיד ירכוש ידע ACS
התלמיד יגדיר שרתי TACACS+ עם מפתחות מוצפנים
התלמיד יגדיר שרתי RADIUS עם מפתחות מוצפנים

נושאים :

אבטחת נתבי קצה
ניהול חיבורים להגדרות נתבים
ניהול והגדרת חיבורים מרוחקים
הגדרת SSH לגישה מרחוק
הגדרות רמות גישה
OOB ושימוש באמצעי LOGGIN
שרתיי SYSLOG , SNMP , NTP
ביקורת חשבונות
נעילת נתבים לאבטחה מבוקשת
שימוש ב SDM לוריפיקציה

משרד החינוך
מינהל מדע וטכנולוגיה
מגמת תקשוב

הגדרת שרת מבוסס AAA

פרק 4 – חומות אש ברשת הבינונית והרחבה

מטרות :

התלמיד ירכוש ידע על עבודה עם ACLs
התלמיד יגדיר ACLs בממשקים CLI ו SDM
התלמיד יגדיר ACLs מבוססות זמנים
התלמיד ירכוש ידע בעצירת התקפות בעזרת ACLs
התלמיד יגדיר CBAS חסימת תכנים ע"י ACLs

נושאים :

הגדרת ACLs סטנדרטי ומורחב על גבי ממשק CLI
הגדרת ACLs סטנדרטי ומורחב על גבי ממשק SDM
הגדרת ACLs מורכבות , Time-Based , Dynamic , Reflective
עצירת מניעת התקפות על ידי ACLs במערכות
טכנולוגיות חומת אש
אבטחת הרשת על ידי חומות אש
הקמת חומת אש בעיצוב הרשת
CBAS חסימת תוכן על ידי ACLs
הפעלת ACLs על ידי Inspection
הפעלת ACLs לפי איזורים מבוססים על נהלי הארגון (ZPF)
הגדרת ZPF על ידי CLI
הגדרת ZPF על ידי SDM
בדיקת חומות האש ופתרון בעיות אפשרי

פרק 5 – מניעת חדירה לרשת המקומית ורחבה

מטרות :

התלמיד ירכוש ידע על מערכות זיהוי פלישה
התלמיד ירכוש ידע על מערכות מניעת פלישה
התלמיד יגדיר מערכות IDS על בסיס CLI ו SDM
התלמיד יגדיר מערכות IPS על בסיס CLI ו SDM

נושאים :

מאפייני IDS ו IPS והבדלים ביניהם
משתמש מבוסס מערכות IPS (HIPS) שימוש ב CSA
רשת מבוססת מערכות IPS (Network-Based IPS)
חתימות IPS (אטומית מול קומפוזיטית)
מאפייני חתימת IPS
אזעקת IPS

משרד החינוך
מינהל מדע וטכנולוגיה
מגמת תקשוב

ניתור IPS
הגדרת IPS על ידי CLI ו SDM
ניתור תקלות במערכות IPS ו IDS
פתרון תקלות במערכות IPS ו IDS

פרק 6 – אבטחת הרשת המקומית

מטרות :

התלמיד ירכוש ידע מערכות Iron Port כאביזר קצה
התלמיד ירכוש ידע במערכות קצה CSA
התלמיד ירכוש ידע בהתקפות LAN מתקדמות
התלמיד ירכוש ידע על עצירת התקפות בשכבת העורק
התלמיד ירכוש ידע בהתקפות VOIP ו SAN

נושאים :

הכרות עם מערכות קצה לאבטחת הרשת
הכרות עם מערכות Iron Port
הכרות עם מערכות NAC ומערכות CSA
הכרות מערכות של חברות שונות
הכרות עם מערכות לאבחון מיילים , אתרים , אבטחה
הכרות עם אבטחה בשכבת העורק (Data Link)
התקפות על מערך ה Spanning Tree Protocol
התקפות מתקדמות ב LAN
התקפות על מערכי VLAN
מצבי אבטחה בשכבת העורק והתמודדות עם התקפות
הגדרת מצב אבטחה Storm Control (SC)
הגדרת SPAN ואבטוח באמצעות SPAN
שילוב SPAN עם IDS ליצירת מראה רשת
מערכות SAN חשיבות ואבטחה
מערכות VOIP חשיבות ואבטחה

פרק 7 – מערכות הצפנה וקריפטולוגיה

מטרות :

התלמיד ירכוש ידע על קריפטולוגיה
התלמיד יכיר את מערכות ההצפנה הקיימות
התלמיד ירכוש ידע על אבטחה באמצעות הצפנות קידודים האשינג בכדי ליצור מערך אבטחה מלא
התלמיד ירכוש ידע על מערכות הצפנה סימטריות ומפתחות משותפים
התלמיד ירכוש ידע על מערכות הצפנה א-סימטריות ומפתחות משותפים

נושאים :

אבטחת חיבורים ברשת המקומית
אבטחה ע״י PIN למשתמש קצה ברשת
תורת ההצפנות (יוליוס קיסר)

משרד החינוך
מינהל מדע וטכנולוגיה
מגמת תקשוב

סוגים של הצפנות לאורך ההיסטוריה
צפנים שונים וסוגי הצפנות קדומות
התקפות ברוטליות לפתיחת צפנים
סטטיסטיקות לסיסמאות לפי מערך תווים
חוקי NSA לגבי הצפנות מידע
סוגי הצפנה ופרוטוקולי הצפנה ואוטנטיקציה וסודיות
הצפנות על ידי האשינג
האשינגעם SHA-1 והצפנה עם MD-5
אוטנטיקציה עם HMAC על מערכות VPN
ניהול מפתחות על ידי שינוי אחסון וריפיקציה משתנה
מפתחות ארוכים ומפתחות קצרים
הצפנות סימטריות ו א-סימטריות
סוגי הצפנה DESAESSEALRCDES3
DSA אלגוריתמים לחתימות דיגיטליות
PKI מפתחות משותפים למרכות אינטרנט
סטנדרטים של PKI וסמכות אישור סטנדרטים
היררכיית סטנדרטים ואישורי סטנדרטים AC

פרק 8 – מערכות VPN (Virtual Private Network)

מטרות :

התלמיד ירכוש ידע על מערכות VPN
התלמיד ירכוש ידע בגדרת VPN
התלמיד ירכוש ידע ב IPSec
התלמיד יגדיר VPN על גבי CLI ו SDM

נושאים :

VPN שימושיו בחברה ובארגונים
התפתחות ה VPN וסטנדרטים שבשימוש ה VPN(MPLS , GRE)
טופולוגיות VPN – גישה מרחוק , אתר לאתר
פתרונות VPN Cisco PIX Firewall 500
פתרונות VPNCisco ASA 5500
פתרונות VPNCisco VPN 3000
פתרונות VPN ב SOHO
פתרונות לקוח ל VPN חיבור מרחוק צד לקוח
תוספות חומרה להאצת VPN (VAC+ , SPA , AIM)
הגדרת VPN על מערך GRE על ידי פתיחת Tunnel על בסיס CLI
היכרות עם סטנדרט IPSec , מערכות IPSec והטמעת IPSec
היכרות על IKE (מפתחות אינטרנט משתנים) ופרוטוקול DH
הגדרת VPN על ידי טופולגית אתר לאתר isakmp על בסיס CLI
יצירת Crypto Map ובדיקת מעבר ופתרון בעיות
הגדרת IPSec על בסיס SDM
הגדרת VPN על בסיס SDM
בדיקת ה VPN ויצירת מערכת שליטה לבקרה לפתרון בעיות
היכרות ויצירת VPN על בסיסי SSL
הגדרת שרת VPN על ידי SDM

משרד החינוך
מינהל מדע וטכנולוגיה
מגמת תקשוב

חיבור צד לקוח לשרת VPN

פרק 9 – ניהול אבטחת רשת מתקדם

מטרות :

התלמיד ירכוש ידע בעקרונות עיצוב רשת מאובטחת
התלמיד ירכוש ידע בניתוח פגיעות רשת
התלמיד ירכוש ידע בניהול סיכוני אבטחה
התלמיד ירכוש ידע במערכות הגנה עצמית
התלמיד יגדיר מערכות NESUS ומערכות פגיעות שונות

נושאים :

בדיקת אבטחת הרשת
ניהול סיכונים וניהול פגיעות תוך חברתיות
הימנעות מסיכונים ובידוד התקפות
מערכות הגנה עצמית על ידי שימוש ב SDN
יצירת מבנה אבטחה
שחזור בטוח במערכות מרשת ומידע
בדיקת מערכות ובדיקות מערכתיות ST&E
בדיקת פגיעות על ידי כלים שונים
בדיקת פגיעות על ידי NMAP
בדיקת פגיעות על ידי SuperScan
הכנת תוכנית המשכיות (Worst Case Scenario) WCS
תוכניות הפרדת גיבויים
מערכות SDLC
תוכנית מערך SDLC
תחזוקה ותפעול SDLC
שילוב מערכות וחלוקת תפקידים באבטחה מרכזית
אבטחה למערכות שונות (מייל , טלפוניה , אפליקציות , אלחוט)
שילוב לקוח , שותפים , עובדים
סטנדרטים קווים מנחים ופרוצדורות
תחומיי אחריות וחוקים ואתיקה מקצועית